その時、会社は動けますか？

IPA「ランサムウェア 被害から学ぶ教訓集」から読み解く
法務・コンプライアンス担当者のための実務対応

－ 経営・個人情報・危機対応・ガバナンスの視点から －

止まる業務	失われるデータ	問われる説明責任	求められる法的対応	試されるガバナンス

弁護士法人 三宅法律事務所

弁護士　渡邉 雅之

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

2　なぜ法務・コンプラ担当者向けに読むのか

ポイント：IT事故ではない

1.　初動で説明責任が顕在化
発覚直後から、顧客・取引先・当局・社内への説明が必要になる。

2.　個人情報対応と同時進行
法26条1項の「漏えい、滅失又は毀損」が同時に問題となる。復元不能な暗号化は毀損に当たる。

3.　経営判断が連続する
停止、復旧、公表、身代金、外部専門家選定を短時間で決める。

本ウェビナーのゴール

「事故後に止める法務」から「事故前に会社を動かす法務」へ
IPA資料全体を、①危機管理、②個人情報保護、③証拠保全、④対外説明、⑤取締役会・監査の5つの実務論点に再構成する。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

3　この報告書の位置づけと読みどころ

資料の位置づけ
・2026年9月8日公表のIPA資料
・国内の被害組織へのヒアリングを基礎にした教訓集
・想定読者は経営者、法務、広報、事業部門、情シス等

読むときの注意点
・包括的・体系的な方法論そのものではない
・個別事案の法的判断ではない
・ただし「実際の被害現場で何に困るか」が具体的

法務・コンプラ担当者に刺さる理由

初動の判断基準　役割分担　個人情報対応　公表・通知　証拠保全　取締役会報告

本日の立ち位置と読み方

私はランサムウェアの復旧現場にいた人間ではありません。個人情報保護法の漏えい等報告実務、業法上の報告、そして監査役・特別委員会の側から、この資料を読みます。

「新しい法的義務ができた」という話ではなく、既存の法務・コンプライアンス実務をランサムウェア前提で作り直す話として聞いてください。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

ランサムウェアは、IT事故ではなく経営危機

暗号化に気づいた時点で、すでに多くの判断が同時発生する

業務停止
受注・出荷・請求・顧客対応が止まる

データ問題
漏えい、滅失、毀損、復元不能が重なる

説明責任
顧客・取引先・当局・社内への説明

経営判断
停止・復旧・公表・身代金方針を判断

法務・コンプラ上の含意
「情報システム部門が復旧してから法務が確認する」では遅い。発覚直後から、事業継続・通知・公表・証拠保全を同時に設計する必要がある。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

5　ランサムウェア事案の特性

発覚時＝最終局面

暗号化に気づく頃には、攻撃者はすでに「侵入・探索・横展開・持ち出し」を終えていることが多い。

初期侵入 → 探索 → 権限取得 → 横展開 → 持ち出し → **暗号化**

ここで気づく

時間的猶予がない	業務停止と復旧判断が同時発生	二重脅迫により暴露リスクも重なる	情シスに負荷が集中しやすい	平時の備えの差が成否を左右

法務・コンプラ上の含意：発覚後に「調べてから決める」時間はない。判断基準を事前に持つ。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。攻撃フェーズは、同資料がMITRE ATT&CK（Tactics）を参考に再構成したものに基づく

6　発覚直後に迫られる「経営判断」の束

ランサムウェア対応では、技術対応と同時に、法務・広報・事業継続の判断が一気に来る。

止める判断	ネットワーク遮断／感染端末切離し／事業停止
戻す判断	復旧方針／バックアップ安全性／再構築か復元か
知らせる判断	当局報告／本人通知／取引先説明／公表
交渉判断	身代金方針／攻撃者接触／警察・専門家連携
守る判断	証拠保全／ログ保全／フォレンジック範囲

重要：これらは「順番に」ではなく「並行して」処理される。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

7　匿名事例①：情シスに全部集まると復旧が止まる

匿名事例 01

「IT事故だから情シスで対応」が最大の落とし穴

何が起きたか

警察相談、個人情報保護委員会への報告、取引先説明、攻撃経路調査、被害分析、復旧方針、復旧作業、再発防止策まで情シスに集中。外部報告を分担しないと復旧が進まないと指摘された。

法務・コンプラの学び

事前の役割分担がなければ、有事に業務を割り振れない。
法務・広報・営業・事業部門を含む横断体制が不可欠。

「インシデント発生時、個人情報保護委員会への報告文と取引先説明の下書きを誰が作るか」は決まっていますか。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

8　有事対応チームは「法務を含む司令塔」で設計する

必要なのは、部署ごとの縦割り対応ではなく、判断と説明を一元化するハブ機能。

経営・事業
- 停止／継続の判断
- 復旧優先順位
- 顧客影響の把握
- 社内向けメッセージ

法務・コンプラ
- 当局報告
- 本人通知
- 契約上の通知義務
- 公表文案
- 証拠保全

技術・外部専門家
- 封じ込め
- フォレンジック
- 復旧
- EDR/SOC
- ダークウェブ監視

設計思想
情シスは復旧に集中させる。法務・コンプラは、外部報告・対外説明・証拠保全・取締役会報告を整理し、会社全体が動ける状態を作る。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

9　匿名事例②：BCPが「地震用」だけでは足りない

匿名事例 02　**人も建物も無事。でもシステムが止まり、業務が止まる。**

何が起きたか
製造業では、生産管理システムが止まると、在庫があっても納品できない。自然災害向けの手作業手順があった組織は、ランサム事案でも対応しやすかった。

法務・コンプラの学び
サイバーBCPでは「システムが使えない状態で、どの業務をどう続けるか」を事業部門と一緒に決める必要がある。

主要業務について「紙・電話・代替クラウド」で何日回せるか、事業部門は答えられますか

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

10　サイバーBCPに入れるべき法務・コンプラ項目

自然災害型BCPに、ランサムウェア特有の「止まる・戻す・知らせる・守る」を組み込む。

業務継続	法的対応	対外説明	証拠保全
・重要業務の優先順位 ・手作業・代替手段 ・復旧後のデータ補正	・委員会・所管官庁への報告 （法26条1項、150条） ・本人通知（法26条2項） ・契約上の通知義務	・取引先説明の順序 ・公表文案 ・問い合わせ窓口	・ログ保全 ・メール・議事録管理 ・フォレンジック範囲

BCP見直しの実務ポイント

・IT部門だけで作らず、事業部門・法務・広報が入る
・「復旧した後の説明」ではなく「止める前からの説明」を設計する
・手作業での継続と、復旧後のデータ補正まで訓練する

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

11　匿名事例③：データ台帳がないと、通知判断ができない

匿名事例 03　**暗号化された後に「何が入っていたか」を調べるのは難しい**

何が起きたか
復旧できないデータがある場合、どの個人データが漏えい・滅失・毀損したのかを特定することが困難。フォレンジックをしても全部は分からないことがある。

法務・コンプラの学び
個人情報管理台帳は、平時の管理資料であると同時に、事故時の説明・報告・通知の基礎資料になる。

暗号化されてサーバに入れなくても、保存されていた個人データの種類・件数・保管部門を説明できますか。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

12　個人情報保護法：報告義務は「件数」から入らない

ランサムウェア事案は、通常、規則7条3号に該当する。本人1件でも報告義務が生じ、確報期限は60日となる。

1　要配慮個人情報

規則7条1号（おそれを含む）

2　財産的被害のおそれ

規則7条2号（決済・口座情報等）

3　不正目的の行為

規則7条3号／ランサムは原則ここ・件数不問

4　本人1,000人超

規則7条4号（行政機関等は100人超）

事象の分類（法26条1項）

漏えい：窃取・ダークウェブ公開。ただし高度な暗号化等の秘匿化措置がある場合は該当しない。

滅失／毀損：暗号化により復元不能となった場合は毀損。

期限（規則8条・10条）

・速報：速やかに（概ね3～5日以内）

・確報：30日以内。ただし3号該当事案は60日以内

・本人通知：状況に応じて速やかに（法26条2項）。困難な場合は代替措置

委託関係（法26条1項ただし書・規則9条）

・委託元・委託先の双方が報告義務者。委託先が委託元に通知すれば委託先の義務は免除

・委託契約に通知の時限・様式・窓口を定めていなければ、この免除規定は機能しない

法務・コンプラの含意

最初に確認すべきは件数ではなく「不正アクセスの可能性」。規則7条3号を前提に60日のカレンダーを引き、逆算で調査スコープを設計する。

「外部送信の痕跡が確認されない」ことは、規則7条各号の「おそれ」を否定しない。調査結果と報告要否は別の判断である。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

13　業法上の報告義務：委員会報告で終わらせない

個人情報保護法上の報告とは別に、業法上の報告・届出が並走する（権限委任につき法150条）。

金融機関

・システム障害の届出（銀行法53条1項、同施行規則35条1項）

・金融庁の監督指針に基づくシステムリスク管理と障害時対応

・金融分野における個人情報保護に関するガイドラインの適用

電気通信・医療・重要インフラ

・電気通信事業者は電気通信事業法28条の報告

・医療機関は「医療情報システムの安全管理に関するガイドライン」に基づく対応

・重要インフラ分野は分野別ガイドラインと所管官庁への報告

契約・開示

・秘密保持契約・業務委託契約上の通知義務と期限

・上場会社は適時開示（東証有価証券上場規程402条2号）

・有価証券報告書「事業等のリスク」の記載

法務・コンプラの実務

報告先・期限・様式を一覧化した「報告マトリクス」を平時に作る。委員会への速報3〜5日・確報60日というカレンダーの上に、業法上の報告が重なる。最も短い期限が全体を規律する。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

14　身代金：支払わない判断も「法的判断」である

論点整理

問題は支払うか否かではなく、その判断をどう根拠づけ、どう残すかにある。

制裁・刑事のスクリーニング

・外為法16条1項：資産凍結対象者への支払等は許可が必要。財務省告示のリストを確認する

・OFAC SDNリスト等の海外制裁リスト。米国関連性があれば域外適用の可能性

・組織的犯罪処罰法10条・11条、テロ資金提供処罰法の適用可能性

・攻撃者の特定は容易でない。ランサムノート、検体、送金先アドレスから推定するほかなく、照合には限界があることを前提に判断する

交渉代行・保険・記録

・交渉／支払の代行を用いる場合、業者の役割・責任範囲・準拠法を契約で明確にする

・サイバー保険の身代金補償は、事前同意条項と制裁除外条項の確認が前提

・支払の有無にかかわらず、報告義務（法26条1項）も本人通知（同条2項）も消えない

・照合結果、外部専門家の意見、決議の過程を議事録に残す。会社法330条、民法644条

公的機関の立場と、決めた後にやること

CRI「GUIDANCE FOR ORGANISATIONS DURING RANSOMWARE INCIDENTS」（2024年）、警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について」（2026年3月）、経済産業省注意喚起（2020年12月18日）は、いずれも支払いを避けるべき方向で一致している。

「払わない」と決めても、攻撃者の連絡経路・ランサムノート・リークサイト情報は保全する。攻撃者グループの特定と、事案収束後のダークウェブ監視に使う。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

15　公表・通知・取引先説明：言葉で二次被害を防ぐ

ランサムウェア対応では、技術復旧と同じくらい「説明の精度」が重要になる。

初報	続報	個別説明	収束時
確認できた事実 業務影響 問い合わせ窓口	調査状況 復旧見込み 影響範囲	取引先別影響 契約上の通知 再開条件	再発防止策 継続監視 新事実の取扱い

避けたい表現
「漏えいはありません」
「完全に安全です」
「近日中に必ず復旧します」

望ましい表現
「現時点で確認された事実」
「調査継続中」
「追加判明時は速やかに説明」

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

16　公表文の読み方：他社のリリースを法務の目で読む

被害公表は公開情報である。第一報から最終報までを並べて読むと、自社のひな型に必要な留保が分かる。

第一報で読むところ

- 確認できた事実と、推測・見込みの切り分け方
- 業務影響をどこまで具体的に書いたか
- 個人情報への言及の有無と、留保の付け方
- 問い合わせ窓口と、次報の時期の予告

続報で読むところ

- 第一報の表現がどこで、どう更新されたか
- 「調査中」から確定に変わった項目は何か
- 件数・データ項目が後から追加されていないか
- 更新の理由を説明しているか

収束時に読むところ

- 「漏えいは確認されていない」の使われ方
- 再発防止策の具体性と、実施時期の記載
- 継続監視への言及があるか
- 新事実が判明した場合の含みを残しているか

社内演習としての使い方

自社と同業種の公表文を3本選び、第一報と最終報を並べて読む。表現がどこで変わったかを追えば、第一報の時点で付けておくべき留保が具体的に見える。IPA資料の匿名事例より、実名の公表文3本を精読するほうが自社のひな型づくりには早い。

出所：各社の公表資料（公開情報）に基づき弊所作成

17　匿名事例⑤：バックアップがあっても復旧できない

匿名事例 05　**「バックアップがあります」では安心できない**

何が起きたか
バックアップが汚染されている可能性があると復旧に使えない。侵入開始時期が特定できなければ、どの時点のバックアップが安全か判断できない。

法務・コンプラの学び
バックアップとログはセットで見る。隔離・保護・復元テスト・侵入時期特定のログ保存が、後の説明責任にも直結する。

「最後に復旧テストをした日」と「その復旧で発生するロールバック業務」は把握されていますか。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

18　証拠保全・ログ確保：後から説明できる会社になる

フォレンジックは「残っているもの」しか見られない。事故後の説明責任は、平時のログ設計で決まる。

保全対象
Firewall
VPN
AD
サーバ
EDR
操作ログ

判断に使うこと
侵入時期
侵害範囲
データ持出し有無
安全な復元時点

法務の関与
保全指示
調査範囲
報告書の表現
開示範囲の管理

ログは「技術担当の記録」ではなく、会社が説明責任を果たすための証拠である。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

19　証拠保全と秘匿性：フォレンジック報告書は誰の文書か

調査報告書は、後の訴訟・行政対応で提出を求められ得る。作成前に用途と宛先を決める。

日本法の前提

弁護士・依頼者間の秘匿特権は原則として認められていない。調査報告書は文書提出命令（民訴法220条4号）の対象となり得る。

報告書の設計

原因分析用と対外説明用で、粒度・宛先・配布範囲を分ける。事実と評価を分離し、断定的な法的結論を技術報告書に書かせない。

米国関連がある場合

In re Capital One（E.D. Va. 2020）では、法務経由で発注しただけではwork product保護が認められなかった。契約目的・費用負担・配布範囲の設計が問われる。

法務が平時に決めておくこと

・保全指示は法務名で、対象・期間・凍結範囲を書面で発出する

・ベンダー契約に、報告書の作成目的・成果物の帰属・第三者開示の可否を規定する

・ベンダーは平時に複数候補を選定しておく。事故後の短期間で信頼関係は築けず、途中交代した例も報告されている

・「何が残るか」を、前スライドのログ設計と一体で先に決める

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

20　AD・MFA・最小権限：契約・監査でも問われる領域

内部ネットワークは安全、という前提は崩れている。攻撃者は権限を取り、横展開する。

Active Directory
侵害されるとユーザー情報取得、端末への一斉配布などが可能になる。

MFA・最小権限
標準ユーザー利用、管理者権限の限定、不要アカウント削除。

ネットワーク分割
侵入後に横展開しにくい構成にし、被害範囲を限定する。

法務・コンプラでの実装場面

・委託先・子会社のセキュリティ条項、監査権、報告義務に落とし込む（委託先の監督＝法25条）

・取引先からのセキュリティ質問票に、実態ある回答ができる体制を作る

・侵入の起点は高度な攻撃より、更新の遅れ・一時的な設定変更の放置といった運用の隙が多い。例外措置と権限付与を「誰がいつ戻すか」まで管理する

・「導入済み」ではなく「運用・監視・例外管理」まで確認する（安全管理措置＝法23条）

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

21　匿名事例⑦：EDRのアラートを見ていなかった

匿名事例 07　EDRは「入れる」より「使える」ことが重要

何が起きたか
暗号化検知のアラートメールは出ていたが、週末深夜だったため管理者がタイムリーに受け取れず、対応が遅れた事例がある。

法務・コンプラの学び
EDR導入だけでは足りない。24時間監視、エスカレーション、停止判断権限、SOC連携、ログ監査まで設計する。

重大アラートが土曜午前2時に出たら、誰が何分以内に確認し、誰に上げる設計ですか。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

22　「漏えいなし」の証明は困難

フォレンジック調査で分かるのは「確認できた事実」。確認できないことを「なかった」とは言い切れない

取引先からよく求められるもの
「弊社データが漏えいしていない証明をください」
「ベンダーの保証書を出してください」
「再開条件として漏えいなしを確認してください」

実務上の正しい向き合い方

断定証明ではなく、調査で確認された事実、未確認事項、継続監視、再発防止策を丁寧に説明する。

「痕跡が確認されない」ことは、規則7条各号の「おそれ」を否定しない。調査結果と報告要否は別の判断である。

取引先が求める「証明」は、表明保証・補償・再開条件の契約条項として処理する。

表現例

避ける
情報漏えいはありませんでした。

使いやすい
現時点の調査では、外部送信を示す痕跡は確認されていません。

平時の暗号化は法的効果を持つ：
高度な暗号化その他の秘匿化措置が講じられた個人データは「漏えい」に該当しないと整理されている（ガイドライン通則編）。セキュリティ投資を法務の言葉で説明できる論点。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

23　海外拠点・子会社：グループで一番弱い場所から入られる

本社と海外拠点・M&A子会社で、MFA・EDR・ログ・法制度・訴訟リスクが異なる。

ITインフラの差

本社ではMFA・EDRを導入済みでも、海外拠点では未導入という差がある。ログ保存期間や監視体制も揃っていないことが多い。

通知期限の差

・日本：速報3～5日／確報60日（規則8条）

・EU：72時間（GDPR33条）

・米国SEC登録：4営業日（Form 8-K Item 1.05）

・中国：遅滞なく（個人情報保護法57条）

ガバナンス・訴訟リスクの差

買収後の統合未了、ローカル運用、委託先管理の不統一が弱点になる。米国では漏えい後のクラスアクションが提起されやすく、フォレンジックと対外公表を慎重に進める必要がある。

法務・コンプラの実務

グループ全体では、最も短い期限が全体を規律する。海外拠点のログ未保存やEDR未導入は、その法域の期限を守れないという法務問題として提起する。M&A・子会社管理・委託先管理のチェックリストにランサムウェア耐性を入れ、契約条項だけでなく運用証跡まで確認する。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

24　取締役の内部統制システム構築義務との接続

ランサムウェア耐性は、会社法上の体制整備義務と開示・監査の問題として整理できる。

体制構築義務	機関設計別	開示・監査	判例が示す水準
取締役会設置会社は会社法362条4項6号、会社法施行規則100条1項2号（損失の危険の管理に関する規程その他の体制）。取締役会非設置会社は348条3項4号。	監査等委員会設置会社は399条の13第1項1号ハ、指名委員会等設置会社は416条1項1号ホ。いずれも取締役会の決議事項とされる。	事業報告における体制の内容と運用状況の概要（会社法施行規則118条2号）。監査役の監査（会社法381条1項）。有価証券報告書「事業等のリスク」、内部統制報告（金商法24条の4の4）。	大和銀行事件（大阪地判平成12年9月20日）、日本システム技術事件（最判平成21年7月9日）。求められるのは「相応の体制」だが、既知の脅威への不作為は別に評価され得る。

法務・コンプラの実務

- 「ランサムウェア対策」を技術予算の議題ではなく、体制整備の決議事項として設計する
- 取締役会への定期報告の枠を作り、判断根拠を議事録に残す
- 事業報告・監査報告に載る水準で、運用状況を説明できるようにする

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

25　2026年改正個人情報保護法：効くのは課徴金ではない

令和8年7月10日成立・7月17日公布。政令・委員会規則・ガイドラインは今後策定される。

まず誤解を解く

・課徴金（改正法148条の3～148条の17）の対象は、対価を得て行われる悪質な類型に限定。利得剥奪型で、売上高比例ではない

・安全管理措置義務（法23条）違反は、中間整理では検討されたが対象から外された。漏えい等報告義務（法26条）違反も対象外

・「漏えいすれば課徴金」ではない。GDPR型の制裁金とは制度設計が異なる

実際に効いてくる3つのルート

・命令のハードル低下：「侵害の切迫性」要件が撤廃され、「重大な権利利益が害されるおそれ」の段階で命令可能（改正法148条2項）。緊急命令も切迫段階で可能（同条3項）

・命令内容の拡張：是正措置にとどまらず、本人への通知・公表その他必要な措置を命じられる（同条1項～3項）

・命令違反の制裁：措置命令違反について法人重科（法人に1億円以下の罰金・改正法185条）

法務・コンプラの含意

問われるのは課徴金ではない

安全管理措置義務（法23条）違反を理由とする命令とその履行が焦点になる。

公表の主導権

自社の判断で公表範囲を決める前提が変わる。主導権を残せるかが分岐点。

団体による差止請求・被害回復制度、プロファイリング規制は今回見送られ、衆参の附帯決議で継続検討とされた。施行時期は公布後2年以内（2028年春～7月頃見込み）。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

26　取締役会・監査役・管理部門が今すぐ確認すべき10問

1	発生時の意思決定者は明確か	6	バックアップは隔離・保護され、復元テスト済みか
2	ネットワーク遮断の判断権限は決まっているか	7	必要なログは十分な期間保存されているか
3	サイバーBCPは整備されているか	8	EDRアラートに土日深夜も対応できるか
4	手作業で継続できる主要業務は特定済みか	9	有事に依頼する専門家候補は決まっているか
5	個人情報を含むデータの所在を把握しているか	10	公表・通知・取引先説明のひな型と体制はあるか

この10問に即答できない場合、ランサムウェア耐性は十分とはいえない。

取締役会設置会社では、これらは会社法362条4項6号・会社法施行規則100条1項2号の体制整備の内容そのものであり、事業報告（同規則118条2号）における運用状況の説明対象となる。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成

27　明日からの実行アクション

完璧な体制を待つのではなく、まず「誰が・何を・いつまでに」確認するかを決める。

30日以内

・有事対応体制と連絡先を整理
・個人情報・重要データの棚卸し
・外部専門家候補の洗い出し

90日以内

・サイバーBCPの見直し
・バックアップとログ保存の点検
・公表・通知・説明文案の整備

半年以内

・演習の実施
・EDR監視体制の高度化
・取締役会への定期報告設計

ランサムウェア対応は、IT部門だけの課題ではない。
法務・コンプライアンス部門が中心となって、経営・事業・情報システムをつなぐ。

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成

～ 本日のまとめ ～

法務・コンプライアンスは、

会社を止める部門ではなく、

会社が動けるように整理する部門。

・発覚時には、すでに最終局面であることが多い

・報告義務は件数ではなく規則7条3号から入る。確報は60日以内

・バックアップ・EDR・ログは「導入」ではなく「使える運用」が重要

・「漏えいなし」は安易に断定しない

・有事の説明責任は、平時の体制・台帳・文案で決まる

出所：IPA「ランサムウェア被害から学ぶ教訓集 ～経営者のためのランサムウェア対策ハンドブック～」（2026年9月8日）を基に作成。法令・条文の解釈に関する記載は弊所作成